IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-11 (Cancelled)

12. (Currently Amended) A system for providing access to restricted use digital software products, comprising:

a server network comprising a server computer, a customer database storing user information, and a content database storing a plurality of software product titles;

a client console operated by a user and configured to playback a selection of the plurality of software titles;

a detachable storage media installable in said client console; said detachable storage media having a data structure thereon comprising at least one [[of a]] user identifier (ID), wherein the server computer distributes a software product to a user of the client console and encrypts the software product using information comprising the user identifier and a purchase option governing use of the software product by the user.

13. (Original) The system of claim 12 wherein the user transmits decryption information to the server computer to provide access to the software product distributed to the user.

14. (Currently Amended) The system of claim 13 wherein ~~the server computer distributes~~ the software product is distributed to the user on a readable disk media.

15. (Original) The system of claim 13 wherein the server computer distributes the software product to the user over a communications link coupling the client computer to the server.

16. (Original) The system of claim 14 wherein the user transmits the decryption information to the server computer using a telephone coupled to the server computer through a public switched telephone network.

17. (Original) The system of claim 15 wherein the user transmits the decryption information to the server computer over the communications link.

18. (Original) The system of claim 13, wherein the purchase option comprises using the software product for a pre-set period of time.

19. (Original) The system of claim 13, wherein the purchase option comprises using the software product for a pre-set period of accesses.

20. (Currently Amended) The system of claim 13 wherein the software product is encrypted using a public key/private key encryption system, and wherein a user public key (User A) is assigned and transmitted to the user and a client console public key (Console A) is assigned and coded in a [[the]] detachable storage media installable in the client console.

21. (Original) The system of claim 13, wherein the client console is an interactive game computer, and the software product comprises an interactive computer game executable by the client console.

22. (Currently Amended) A server computer configured and adapted to be coupled to one or more client computers over a communications network, the server computer comprising:

a customer database configured and adapted for storing user information, and a content database storing a plurality of software product titles;

a distribution module configured and adapted for distributing a software product from the plurality of software product titles to a user of a client computer of the one or more client computers upon request of the user;

an encryption module configured and adapted for encrypting the software product using information comprising a user identifier (ID) and a purchase option governing use of the software product by the user; and

a decryption module configured and adapted for receiving decryption information from the user and providing access to the software product upon confirmation of the decryption information.

23. (Currently Amended) The server computer of claim 22, wherein the purchase option comprises one of:

using the software product for a pre-set period of time, and using the software product for a pre-set ~~period~~ number of accesses.

24. (Currently Amended) The server computer of claim 23 wherein the software product is encrypted using a public key/private key encryption system, and wherein a user public key (User A) is assigned and transmitted to the user and a client console public key (Console A) is assigned and coded in a [[the]] detachable storage media installable in the client console.

25. (Original) The server computer of claim 24, wherein the client computer is an interactive game computer, and the software product comprises an interactive computer game executable by the client console.

26. (Original) The server computer of claim 25 wherein the software product and decryption information are transmitted between the server computer and client computer over the communications network.

27. (Currently Amended) The server computer of claim 25 wherein the software product is distributed to the client computer on a readable disk media accessible by the client computer, and wherein the decryption information is communicated to the server computer by the user over a telephone system.

28-53 (Cancelled)

54. (New) A method for distributing a software product, comprising the steps of:

encrypting said software product;

distributing said encrypted software product to a user;

establishing two-way, public key/private key encrypted, secure communication between a product distributor and said user; and

communicating, via said secure communication, data (Title B) enabling decryption of said encrypted software product from said product distributor to said user.

55. (New) The method of claim 54, further comprising the steps of:

communicating purchase information from said user to said product distributor; and

communicating, responsive to said purchase information and via said secure communication, an electronic token from said product distributor to said user that permits said user to use said decrypted software product in a restricted manner.

56. (New) The method of claim 55, wherein said use in a restricted manner constitutes use for a bounded period of time or use for a predetermined number of usages.

57. (New) The method of claim 54, wherein said encrypting of said software product is carried out using a public key (Title A) of a first public key/private key pair that is separate from the public key/private key pairs of said secure communication.

58. (New) The method of claim 57, wherein said data enabling decryption of said encrypted software product is a private key of said first public key/private key pair.

59. (New) The method of claim 54, wherein said establishing of secure communication comprises:

generating, at said product distributor, a second public key/private key pair (User A, User B);

communicating said second public key to said user;

generating, at said user, a third public key/private key pair (Console A, Console B);

encrypting, at said user, said third public key using said second public key; and

communicating said encrypted third public key to said product distributor.

60. (New) The method of claim 59, wherein said second public key/private key pair is created using user information (ID) provided by said user to said product distributor.

61. (New) The method of claim 59, wherein said third public key/private key pair is created using hardware identification means, a hardware identification device or a media identifier of a medium on which said encrypted product has been distributed.

62. (New) The method of claim 61, wherein an execution of said software product on a user's computer requires connection of said hardware identification device to said user's computer.

63. (New) The method of claim 54, wherein any of said communication or said secure communication from said user to said product distributor is effected via touch-tone signals or voice over a public switched telephone network.

64. (New) The method of claim 54, wherein any of said communication or said secure communication from said product distributor to said user is effected via voice synthesis or voice over a public switched telephone network.

65. (New) An article of manufacture embodying a program of instructions executable by a machine, the program of instructions configured and adapted for execution on a content provider server, the article of manufacture including instructions for:

encrypting a software product;

establishing, in conjunction with a reception of counterpart communication originating from a remote client console, two-way, public key/private key encrypted, secure communication between said content provider server and said client console; and

communicating, via said secure communication, data (Title B) enabling decryption of said encrypted software product to said client console.

66. (New) The article of manufacture of claim 65, further including instructions for:

receiving purchase information from a user; and

communicating, responsive to said purchase information and via said secure communication, an electronic token to said client console that permits use of said decrypted software product in a restricted manner.

67. (New) The article of manufacture of claim 66, wherein said use in a restricted manner constitutes use for a bounded period of time or use for a predetermined number of usages.

68. (New) The article of manufacture of claim 65, wherein said encrypting of said software product is carried out using a public key (Title A) of a first public key/private key pair that is separate from the public key/private key pairs of said secure communication.

69. (New) The article of manufacture of claim 68, wherein said data enabling decryption of said encrypted software product is a private key of said first public key/private key pair.

70. (New) The article of manufacture of claim 65, further including instructions for distributing said encrypted software product via a network.

71. (New) The article of manufacture of claim 65, wherein said establishing of secure communication comprises:

generating a second public key/private key pair (User A, User B);

communicating said second public key to said client console;

receiving, as said counterpart communication, a public key of a third public key/private key pair (Console A, Console B) encrypted using said second public key; and

decrypting said encrypted third public key using said second private key.

72. (New) The article of manufacture of claim 65, wherein said reception of counterpart communication originating from said remote client console comprises receiving touch-tone or speech signals over a public switched telephone network.

73. (New) The article of manufacture of claim 65, wherein any of said communication comprises a generation of voice synthesis data for communication thereof over a public switched telephone network.

74. (New) An article of manufacture embodying a program of instructions executable by a machine, the program of instructions configured and adapted for execution on a client console, the article of manufacture including instructions for:

receiving an encrypted software product;

establishing, in conjunction with a reception of counterpart communication originating from a remote content provider server, two-way, public key/private key encrypted, secure communication between said content provider server and said client console; and

receiving, via said secure communication, data (Title B) enabling decryption of said encrypted software product from said content provider server.

75. (New) The article of manufacture of claim 74, further including instructions for:

receiving, via said secure communication, an electronic token to said client console that permits use of said decrypted software product in a restricted manner.

76. (New) The article of manufacture of claim 75, wherein said use in a restricted manner constitutes use for a bounded period of time or use for a predetermined number of usages.

77. (New) The article of manufacture of any of claim 74, wherein said data enabling decryption of said encrypted software product is a private key (Title B) of a first public key/private key pair that is separate from the public key/private key pairs of said secure communication.

78. (New) The article of manufacture of claim 74, wherein said reception of said encrypted software product is effected via a network.

79. (New) The article of manufacture of claim 74, wherein said establishing of secure communication comprises:

receiving, as said counterpart communication, a public key of a second public key/private key pair (User A, User B) from said content provider server;

generating a third public key/private key pair (Console A, Console B);

encrypting said third public key using said second public key; and

communicating said encrypted third public key to said content provider server.

80. (New) The article of manufacture of claim 74, wherein said secure communication comprises displaying said encrypted public key on a display device.

81. (New) A client console for execution and/or reproduction of a software product, comprising:

means configured and adapted for receiving an encrypted software product;

means configured and adapted for establishing, in conjunction with a reception of counterpart communication originating from a remote content provider server, two-way, public key/private key encrypted, secure communication between said content provider server and said client console; and

means configured and adapted for receiving, via said secure communication, data (Title B) enabling decryption of said encrypted software product from said content provider server.

82. (New) The client console of claim 81, further comprising:

means configured and adapted for receiving, via said secure communication, an electronic token to said client console that permits use of said decrypted software product in a restricted manner.

83. (New) The client console of claim 82, wherein said use in a restricted manner constitutes use for a bounded period of time or use for a predetermined number of usages.

84. (New) The client console of claim 81, wherein said data enabling decryption of said encrypted software product is a private key (Title B) of a first public key/private key pair that is separate from the public key/private key pairs of said secure communication.

85. (New) The client console of claim 81, wherein said reception of said encrypted software product is effected via a network.

86. (New) The client console of claim 81, wherein said establishing of secure communication comprises:

receiving, as said counterpart communication, a public key of a second public key/private key pair (User A, User B) from said content provider server;

generating a third public key/private key pair (Console A, Console B);

encrypting said third public key using said second public key; and

communicating said encrypted third public key to said content provider server.

87. (New) The client console of claim 81, wherein said secure communication comprises displaying said encrypted public key on a display device.